REMARKS

Applicants have carefully considered the office action dated July 12, 2003. This response is believed to address all issues and place the application in a condition for allowance.

Non-delivery of the Office Action by the US Postal Service

Applicants hereby report that the office action was never delivered to them; rather on or about November 6, 2003, Applicant Chaganti voluntarily called the Examiner to find the status of the application, which was to have been allowed by then. It turns out that on or about June 14, 2003, another office action rejecting most of the claims was mailed, but to the Kendall Avenue, Palo Alto, CA address. Apparently when the U.S. Post Office returned that office action to the PTO, the PTO sent another office action on or about July 12, 2003 to the Sheridan Avenue, Palo Alto, CA address. By then Applicant Chaganti has provided a change of address with the U.S. Postal Service the Los Angeles, CA address, and he never received the July 12, 2003 office action. Applicant also filed his change of address associated with his Customer Number 24490 and with the Office of Enrollment and Discipline based on his registration with the USPTO.

After numerous conversations with the PTO Customer Service and Examiner Darrow, Applicant could not receive a copy of the office action in time to meet the deadline for filing late by one month. On or about November 14, 2003, Applicant Chaganti, unable to reach Examiner Darrow, left a voice mail message to the Supervisory Examiner, Mr. Gilberto Barrón, Jr., requesting him to assist in sending a copy of the office action by fax. About a week later, on 11/18/2003, Examiner Darrow sent the office action via fax. Applicant thanks Examiners Barrón and Darrow for the courtesy. But the issue of whether the late-filing fee is to be paid in view of the confusion with the mailing is still unresolved. Applicants request Examiner Darrow to refund the petition fee for extension of time, and consider the instant filing as timely filed.

Request to Assign this Case to Customer Number **24490**

Please assign this case to Customer Number **24490** and direct all future correspondence to the address associated with that Customer Number. That number is assigned to the Law Offices of Naren Chaganti.

Finality of this Office Action

The Office Action stated that because the amendments necessitated a new search, the first action was final. But this is not the practice. See M.P.E.P. § 706.07(a).

> A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations which should reasonably have been expected to be claimed. See MPEP § 904 et seq. For example, one would reasonably expect that a rejection under 35 U.S.C. 112 for the reason of incompleteness would be replied to by an amendment supplying the omitted element.

Here, responsive to the Request for Continued Examination, the rejection was made final. Applicant requests reconsideration of the decision to make this action final, because the references cited by the Examiner are not new, they have been cited earlier in this case, and the newly added claim is something that is reasonably expected to be claimed. Moreover, the Examiner, in a telephone interview, suggested that the claim 3 would be allowable if it excluded an executable application in view of Bowman-Amuah, which is the same reference that the examiner used to reject that claim once again, and this time in a final rejection. Applicant requests reconsideration of this rejection.

Formal Drawings

Applicants have already sent formal drawings by mail. Because the office action indicates that it was not received, another copy will be mailed separately.

Rejection of Claim 1 under 102(e) based on Fortenberry

The Office Action rejected claim 2 under 35 U.S.C. § 102(e) as being anticipated by Fortenberry USP 6,005,939 A. Applicants cited Fortenberry in an Information Disclosure Statement filed with the parent application on January 7, 2000. Applicants respectfully traverse this rejection for the following reasons. Claim 2 recites as follows.

step for associating with each information object at least one of a plurality of security clearance levels, thereby enabling access to individually selected portions of the user's personal information;

step for recording each information object and the associated security clearance level(s), said security clearance level(s) being at any granularity;

Fortenberry does not disclose or suggest these steps. Instead, Fortenberry states as follows.

> The passport 304 includes a second field corresponding to a security level field 306. A security level is assigned to each item of user information included in the passport data field 305. Thus, for example, if data in field 305 is assigned a security level of 0 then the data is clear. Alternatively, if the data is assigned a security level of 1 then the data is secured via a security technique such as an encryption technique. The passport 304 also includes a key field 308. One or more keys for encryption and decryption may be stored in key field 308.
>
> Referring to FIG. 4, a flow diagram illustrating the process steps to create a passport is shown. Coding of the process steps of the flowchart of FIG. 4 into instructions suitable to control the computer systems in the passport agent 216 and the user system 208 will be understood by those having ordinary skill in the art of programming. First, the user sends a request to generate a passport to passport agent 216, as illustrated by process step 400. The passport agent receives the request, as illustrated by process step 402, and opens a secure communication channel between the passport agent and the requesting user, as illustrated by process 404. Passport agent 216 then presents to the user a series of queries which may be in the form of menus, as illustrated by process block 406. In response, the user enters the requested information such as social security number, drivers license number, etc., and a corresponding level of security to protect the information item, as illustrated by process blocks 408 and 410. The user specified information is referred to herein as user information or environmental variables. The security levels assigned to each item of user information or environment variables range from highly secure to public. For example, particularly sensitive information may be designated as highly secured and assigned a high security level of 100 on an exemplary scale of 0-100 levels. Less sensitive information may be designated as less secured or even public and assigned a lower security level approaching or equal to zero. Next, passport agent 216 provides a public key to the user to access the passport data, as illustrated by process 418. Finally, the user's information which collectively comprises the Internet passport is stored

and maintained in a highly secured server site on the Internet which serves as the passport agent and guarantees the integrity of the users passport, as illustrated by process block 420.

Security keys are delivered to the passport requestor also in a secure manner. As mentioned above, several security keys may be given to a user, such that access to information may be granted at various levels such as real-ID (very secure), virtual-ID and less private information classes. In this manner, the passport agent protects the passport information provided by the user.

When the passport agent sends passport information to the web server on behalf of the passport holder, the private key is used to encrypt the specific information authorized by the passport holder. When the vendor's server receives passport data from the passport agent, one of the public keys sent by the user is used to unlock the passport data. If the public key does not unlock the passport data, the vendor's server simply ignores the users request.

A security level is also used to assign an encryption key based on a user's password. The encryption method uses the concept of public and private keys so that the public key is given the user to access passport data and the passport agent presents the encrypted user data based on the private key. No one but the passport agent on the Internet has access to the private key. The passport owner has a copy of the public key.

Referring now to FIG. 5, a flowchart illustrating the process steps for providing access to a users internet passport via passport agent is illustrated. The coding of the process steps of the flowchart of FIG. 5 into instructions suitable to control passport agent 216, web site 210 and user 208 will be understood by those ordinary skill in the art of programming. First, the user requests a transaction with a particular vendor, i.e., web site 210, as illustrated by process block 502. Next, the user provides a public key to the vendor, as illustrated in process block 504. The public key was previously provided to the user by passport agent 216. Next, the user requests that passport agent 216 send the user's passport to the vendor, as illustrated by process block 506. This message is encrypted with a security key obtained by the user via a secured method. The vendor requests relevant information contained in the user environment variables from the passport agent, as illustrated by process block 508. The request for information is specified in the message as follows: RELEASE-TYPE TO INTERNET-SITE ON BEHALF OF MY-USER-ID. For example, when requesting the passport agent to release social security number information, the message looks like: RELEASE SOCIAL-SECURITY-NUMBER TO WEB-SITE-X ON BEHALF OF MY-USER-ID. Passport agent 216 receives the request for the information, as illustrated by process block 510 and, based on the security level of the identified information, determines whether or not the requested information should be transmitted to the vendor in encrypted form, as illustrated by decisional block 512. If

the information is to be encrypted, an encryption process is carried out by passport agent 216, as illustrated by process block 514.

Col. 7, line 24 - Col. 8, line 53.

The office action relied on the cited portions to argue that the cited language anticipated the instantly rejected claim 2. However, there is no mention of the assignment of security levels at any granularity, and further, Fortenberry does not state that the security levels can be assigned so as to allow individually selected portions of the information objects to be released to different receiving parties. There are other differences between Fortenberry and the instant application. Because these features clearly distinguish the instantly rejected claims from Fortenberry, all the claims so rejected under 102(e) are believed to be patentable. Further, because claim 2 is believed to be patentable, all claims dependent on claim 2 are also believed to be patentable. Reconsideration is respectfully requested.

Rejection of Claim 2 under 35 U.S.C. § 102(e) - Ho

The office action rejected claim 2 under 35 U.S.C. §102(e) based on Ho, USP 6,148,642 A. But Ho does not teach or suggest the steps of

step for associating with each information object at least one of a plurality of security clearance levels, thereby enabling access to individually selected portions of the user's personal information;

step for recording each information object and the associated security clearance level(s), said security clearance level(s) being at any granularity;

Nothing in Ho discusses a security level. Applicants have stated this in a prior argument. Nothing in Ho further discusses assigning security levels to objects at any granularity in order to enable access to individually selected portions of the user's personal information. Accordingly, it is respectfully submitted that Ho cannot anticipate or render obvious the instantly recited claim 2.

Rejection of Claim 3 under 35 U.S.C. § 102(e) - Bowman-Amuah

Claim 3 recites the following steps.

accessing a second computer coupled to the network, the second computer having an item of interest, said item of interest being other than an executable application;

dragging and dropping the item of interest into the storage area; and

assigning at least one of a plurality of security levels at any granularity to the item of interest.

Bowman-Amuah does not teach or suggest this. In fact, as stated above, the Examiner agreed in a telephone interview that Bowman-Amuah does not teach or suggest dragging and dropping an object other than an executable application, and for that reason this claim was allowable. Yet the office action states that it is rejected for the same reason. Reconsideration is requested.

Rejection of claim 1 under 35 U.S.C. §103(a) based on Bowman-Amuah in view of Yoshida

The office action rejected claim1 as obvious based on a combination of Bowman-Amuah in view of Yoshida (USP 5,767,853). Though the office action states that Bowman-Amuah discloses conditional access authorization, such is not found in that patent. The office action later stated that Yoshida disclosed dragging and dropping an item of interest other than an executable application. But there is no motivation or suggestion from the references themselves, that they could be combined in the manner combined in the office action. Therefore, it is respectfully submitted that the combination would not have been obvious to one of ordinary skill in the art.

Conclusion

In view of the foregoing amendments and remarks, the present set of claims is believed to be in a condition for allowance. Applicants request an early notice of allowance.

Respectfully Submitted,

By:_____
Naren Chaganti (44,602)
432 S. Curson Ave, Ste. 12 H
Los Angeles, CA 90036
naren@chaganti.com E-mail
(650) 248-7011 phone
Attorney for Applicants

Certificate of Faxing

I certify that on the date shown below the foregoing was faxed to (703) 746-7239.

Date: December 12, 2003

By:_____
Naren Chaganti (44,602)